

RECEIVED
CENTRAL FAX CENTER

AUG 18 2006

Appln No. 09/692,747
Amdt date August 18, 2006
Reply to Office action of May 18, 2006

REMARKS/ARGUMENTS

Claims 1, 2, 4, 6-16, 18-30, 32-38, and 40-47 are pending. Claims 1, 4, 6-9, 12, 16, 18, 20-23, 29, and 37 are amended; claims 3, 5, 17, 31 and 39 are canceled; and new claims 46-47 are added.

Claims 1-5, 7-19, 21-31, 33-39 and 41-45 are rejected under 35 U.S.C. Section 103(a) as being unpatentable over Sudia, U.S. Patent 6,009,177 (hereinafter "Sudia"). Claims 6, 20, 32 and 40 are rejected under 35 U.S.C. Section 103(a) as being unpatentable over Sudia in view of Ote et al, U.S. Patent No. 6,023,506 (hereinafter "Ote"). Reconsideration and withdrawal of the rejections of these claims are respectfully requested.

Amended independent claim 1 includes, among other limitations "a client system for generating secret information specific to a first computer used by the user for registering with the on-line system, wherein the secret information includes a hash message authentication key (HMK) and the HMK is encrypted," "a server system capable of communicating with the one or more computers over the computer network for receiving user information and the secret information including the encrypted HMK from the first computer and storing the secret information including the encrypted HMK, wherein the server system decrypts the encrypted HMK to authenticate the user and the first computer," and "a re-registration user interface for requiring the user to re-register when the secret information including the encrypted HMK generated by the first computer is not the same as new secret information including an encrypted second HMK generated by a second computer not the same as the first computer."

Sudia does not teach or suggest the above limitations. Sudia is directed to a key escrow system for "splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users, . . . enforced by a chip device that also self-certifies." Sudia's system is fundamentally different from the claimed invention. For example, the system of Sudia encrypts or decrypts only if a valid sender certificate and a valid recipient certificate are input and a valid Message Control is generated by the sender and validated by the recipient. (Col. 11, lines 3-15).

Appln No. 09/692,747
Amdt date August 18, 2006
Reply to Office action of May 18, 2006

There is no suggestion in Sudia about "a client system for generating secret information specific to a first computer used by the user for registering with the on-line system, wherein the secret information includes a hash message authentication key (HMK) and the HMK is encrypted."

Furthermore, there is no suggestion in Sudia about "a re-registration user interface for requiring the user to re-register when the secret information including the encrypted HMK generated by the first computer is not the same as new secret information including an encrypted second HMK generated by a second computer not the same as the first computer." Instead, in the system of Sudia if the certificate is not valid, the user needs to obtain a new certificate from the escrow center and thus requiring the user to go through the entire process of obtaining a new certificate.

As a result, amended claim 1 is patentable over Sudia. Amended claim 29 includes similar limitations and therefore is also patentable over Sudia.

Amended independent claim 16 includes, among other limitations "generating secret information specific to a first computer used by the user for registering with the on-line system, the secret information including a hash message authentication key (HMK)," "generating a second secret information including a second HMK specific to [a] second computer," "comparing the stored secret information including the HMK specific to the first computer with the received second secret information including the second HMK specific to the second computer," and "requiring the user to re-register with the on-line system responsive to a mismatch between the stored secret information including the HMK and the received second secret information including the second HMK secret key."

As explained above, Sudia does not teach or suggest the above limitations. Accordingly, amended claim is also patentable over Sudia. Amended claim 37 includes similar limitations and therefore is also patentable over Sudia.

Additionally, new dependent claims 46 and 47 include the additional limitation of "receiving a passphrase from the user to authenticate the user and the second computer." This is when the stored first secret information does not match the second secret information because the

Appln No. 09/692,747
Amdt date August 18, 2006
Reply to Office action of May 18, 2006

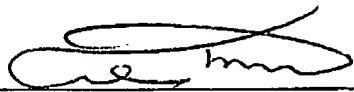
user is using a second computer different from the first computer. In order to authenticate the first computer, the user is required to input a passphrase so that the server would be able to authenticate the user and the second computer.

In short, independent claims 1, 16, 29 and 37 recite a patentable subject matter over cited references. Dependent claims 2, 4, 6-15, 18-28, 30, 32-36, 38, and 40-45 depend from claims 1, 16, 29 and 37, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By



Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS695900.1-*08/18/06 4:52 PM